TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

1401 Wilson Boulevard
Suite 1100
Arlington, VA 222094
P 703.522.5055

Testimony of

Philip J. Bond
President and CEO
TechAmerica

on

Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities

Presented to the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee

February 25, 2010

Chairwoman Sanchez, Ranking Member Miller and Members of the Subcommittee, I am Phil Bond and I serve as President and CEO of TechAmerica.[1] TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity, growth and jobs creation in the United States, as well as the foundation of the global innovation economy. Representing approximately 1,200 member companies of all sizes and 16,000 more through an affiliation with the 40 local and regional technology groups belonging to the Technology Councils of North America, TechAmerica is the industry's largest advocacy organization. Collectively, our companies employ millions of America workers serving the public and commercial sectors of the economy.

We are pleased to present to you today the technology sector's perspective on the various aspects of Department of Defense (DoD) Information Technology (IT) and Cyber security activities. TechAmerica shares with the panel Members here today the goal of improving the security of our nation through the use and deployment of technology to every aspect of our National Security apparatus, from the back offices of the Pentagon to the warfighter in the battlefield. We are also committed to protecting the critical networks and infrastructure of our nation from attacks and disruption. The committee posed several questions to inquire about industry perspectives on information technology and cybersecurity activities and, because these are such expansive topics, I will divide my comments into two sections.

Information Technology

IT Acquisition

TechAmerica believes that we should place emphasis on reform of the IT acquisition processes used at the Department, and for that matter, the entire Federal government. Not doing so threatens the technological edge our warfighters have because of the inability of current processes to keep up with the pace of innovation. Our adversaries both in the battlespace and in cyberspace are not hindered by the red

[1] TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. Representing approximately 1,500 member companies of all sizes from the public and commercial sectors of the economy, it is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Association (GEIA). Learn more at www.techamerica.org.

DRAFT

tape slowing DoD technology acquisitions. To quote Deputy Secretary of Defense Bill Lynn:

> "…[W]ith IT, technology changes faster than the requirements process can keep up. … It changes faster than the budget process and it changes faster than the acquisition milestone process. For all these reasons, the normal acquisition process does not work for information technology."[2]

While such conditions are the result of many factors – ranging from the perpetuation of Cold War-era acquisition policies developed at a time when most technology was not even thought of yet to the drawdown of the acquisition workforce – they need our attention now to make sure that America does not lose its technological advantage.

TechAmerica was asked by the sister panel to this Subcommittee, the Defense Acquisition Reform Panel (DARP), to offer suggestions regarding IT Acquisition and I attach a copy of those suggestions to my testimony for your review and action. We identified four areas where we thought the Armed Services Committee would be able to contemplate and propose legislative solutions.

These are: Acquisition Workforce for IT, Budget Flexibility for IT Programs, Development and Management of Major Automated Information Systems, and Access to Commercial IT Products and Services.

- Acquisition Workforce for IT. DoD does not currently have sufficient organic acquisition resources and capabilities to effectively acquire information technology. In addition to other on-going acquisition workforce enhancement efforts, TechAmerica believes that the Department should establish a cadre of acquisition professionals dedicated solely to the acquisition of information technology products, services and systems. This practice is common in commercial companies that acquire large volumes of complex IT products, services, and systems. Such specialists develop and maintain a thorough knowledge of the products they acquire and an understanding of their companies' purchasing processes. Conversely, government procurement professionals are expected to be proficient in their knowledge of the acquisition rules and regulations that guide their actions.

[2] Defense IT Acquisition Summit, November 12, 2009

- Budget Flexibility for IT. Unfortunately, the acquisition approach for acquiring major automated information systems (MAIS) is beginning to mirror the more traditional MDAP acquisitions. While one can debate whether overseeing and managing large MAIS programs in a manner similar to MDAPs is desirable or not, the need to rapidly acquire information technology to meet warfighters needs in an era where technology cycles are measured in months rather than years is more comparable to rapid contingency contracting than to a traditional MDAP acquisition.

  Successful rapid acquisition requires flexibility in budgeting, as there is no time to wait years to program for funds under the current budget process. By the time funds are obtained to start a program, technology may have leapfrogged by two generations calling into question the approach taken in the original request. Addressing this funding dilemma is critical if DOD is going to leverage the rapid changes occurring in the information technology sector. Combatant commanders should have the ability (not contingent on an ongoing war) to rapidly tap into funding sources for information technology to meet urgent needs of the warfighter.

  Moving beyond the immediate needs of the combatant commanders, the need to refresh technologies and implement a more incremental IT acquisition approach also requires a more flexible budgeting approach. One such approach was outlined by the Defense Science Board in its March 2009 report on the Acquisition of Information Technology as "level of effort" funding. However, current "color of money" issues that distinguish between R&D, Procurement, MILCON, and O&M funds will make it difficult to implement "level of effort" funding, make little sense in funding incremental IT operations and modernization and serve as a barrier to successful IT acquisition.

- Improving the Way DoD Develops and Manages Major Automated Information Systems. As noted above, the government workforce needs material improvement that will take years, not months. In the meantime, the government must continue to acquire IT. TechAmerica recommends three actions that can be taken to improve the process during these years of transition and beyond in the most difficult IT procurements, large transformative IT programs. These are:
  - Authorize the creation of an expert panel to provide objective, professional oversight. This panel would be called upon to provide reasoned, professional assistance and oversight when necessary and give government employees making such judgments protection from second-

DRAFT

guessing by various oversight bodies. Drawn from a pool of respected and objective leaders in IT program management and business transformation, 3-member panels would engage when a program determined that expert help was needed or an oversight entity questioned the appropriateness of IT-related decisions.

- IT Projects should be Limited in Scope, but Scalable to Serve as Solid Foundations for Following Phases. We support the Defense Science Board's (DSB) recommendation that IT projects be limited in scope to simplify the procurement and to allow functionality to be added in useful increments. Called spiral development by the DSB, TechAmerica would place more emphasis on designing each segment or phase to schedule and cost that the DSB might.

  As noted by the DSB and the Acquisition Advisory Panel, DoD and the government as a whole has a requirements development process that needs vast improvement. For IT procurements, the requirements process is not quick enough to stay current with advances in technology. Thus, expecting requirements to accurately capture the technology available in the time the work is done is unrealistic. Until the government workforce that defines IT requirements gets the resources and training required and gains necessary experience, there is little question that requirements may need to be changed and likely scaled back during a program, to meet schedules and budgets.

- Focus on Program Level Engagement First. TechAmerica endorses the DSB's call for "enhanced stakeholder engagement," but would focus immediately on engagement at the program level, building toward enterprise level engagement. We further recommend that selected major IT programs would have assigned during the initial concept development phase and continuing through delivery under the contract, a single manager with a dedicated, stable team representing all major stakeholders. For example, when the Department of Defense intends to acquire an IT system directly affecting warfighting, the team would include at least: (1) the Combatant Commands; (2) DoD or Service CIO office; (3) the Comptroller; (4) government relations; (5) DCAA[3] (6)

[3] This is a significant departure from normal separation of program and audit functions but the assigned auditor could be from a different branch or a different audit organization from DCAA. Costing and pricing considerations need to be represented but not so as to bind subsequent auditors.

DRAFT

Acquisition office; (7) the affected service (if it is a joint program, representatives from each affected service.); (8) Logistics, if there would be any material impact on logistics (many IT programs are delivered and then maintained through hardware and software updates with little other logistical impact); and (9) other stakeholders, such as CECOM if communications were being modified.

- Restore and Enhance Access to Commercial IT Products and Services. We note that it is widely recognized that IT technology refreshment cycle times are turning over much more rapidly than in the past, certainly far more quickly than is the case for major weapons systems. Yet, the acquisition processes used to acquire IT systems and major weapons systems fundamentally are the same. Additionally, the Department (and the Federal government as a whole) has seen a significant decrease in its influence in the Commercial IT market space. DoD, by far the department with the largest IT budget[4], accounts for slightly more than .1% of dollars spent globally on IT[5]. Its presence is further diluted because of the decentralization of buying activities for commercial IT. Indeed, although DoD spends a considerable amount of its budget on IT, the average contract action has declined in size from nearly $2.5M in 2000 to $204K in 2007[6]. This reduction in size and the corresponding decentralization of buying activity also reflect the reality that DoD and the Federal government also have diminished influence on the innovations that are introduced in the commercial market, as well as the functionality that those innovations incorporate.

  The last two decades have brought a significant amount of statutory and regulatory change to the acquisition of products and services for Government use, including the enactment of laws such as the Federal Acquisition Streamlining Act of 1994 (FASA), the Federal Acquisition Reform Act of 1996 (FARA), and the Services Acquisition Reform Act (SARA). The main thrust of these statutes and other broad acquisition reform tools has been to enable a transition in the federal acquisition space from a system based on Government unique requirements under strict design specifications to one centered on the acquisition of commercial items to meet the Government's needs.

[4] FY2011 Budget Submission by President Obama, DoD request is $36.5.

[5] Gartner Says Worldwide IT Spending to Grow 4.6 Percent in 2010

[6] Structure and Dynamics of the U.S. Federal Professional Services Industrial Base, 1995-2007, Center for Strategic and International Studies, February 2009

DRAFT

Like all large institutional processes growing to maturity, however, FAR Part 12 has become burdened with added regulatory and process requirements over time, resulting in the layering of more formal acquisition processes onto the framework of commercial item acquisition (for example, cost element documentation requirements). This has led to a reduction in the efficient use of commercial item acquisition. This impact has been felt most acutely and notably in the ability of the Department and government as a whole to acquire commercial Information Technology (IT) products, services and systems at a pace timely enough to meet government's requirements and still be state of the art.

To the extent that such government acquisition processes vary from those found in the commercial marketplace, they serve as a real and significant deterrent for entry into the Federal market, particularly for small- and mid-sized businesses that frequently do not have the resources to pursue opportunities because of the compliance burden. Some of the government unique acquisition requirements include, but are not limited to: False Claims Act, Trade Agreements Act, Cost Accounting Standards, Truth in Negotiations Act, Audits by the General Accountability Office (GAO) and the Defense Contract Audit Agency (DCAA), suspension and debarment, Administrative Contract Oversight, organizational and personal conflicts of interest, constrained dialogue, bid protests and the delays they cause within the process.

TechAmerica recommends that Congress take a fresh look at IT Acquisition with the creation, funding and staffing of an IT Acquisition review panel similar to the DoD Advisory Panel on Streamlining and Codifying Acquisition Laws (the Section 800 Panel). That panel, funded administratively and staffed with a cross-section of recognized experts from industry and government, embarked on a comprehensive review of the entire acquisition system and yielded the recommendations that led to many of the reforms embodied in the Federal Acquisition Streamlining Act and the Clinger-Cohen Act. We believe the process would be well served by a similar exercise for IT Acquisition.

Finally, we have identified three acquisition models for consideration by the Subcommittee as pilots that could improve the way we acquire IT. These are: the traditional design-bid-build approach for construction authorized under the Brooks Architects-Engineers Act; the two-phase design-build construction procurement process implemented under FAR subpart 36.3; and, a Joint

DRAFT

Solutions Procurement Process used by the Canadian province of British Columbia to acquire sophisticated IT systems. TechAmerica believes all three hold promise as ways that DoD and the Federal government can reform the options for efficient and timely acquisition of information technology.

Science, Technology, Education and Math (STEM) training

TechAmerica is fully aware of the very concerning decline in STEM-educated graduates and is concerned that we are not doing enough to ensure a pipeline of graduates in these critical disciplines. Such a decline threatens our innovation economy and standing in the global marketplace. Studies have identified that our society and culture have lost the challenges for educational excellence that emerged as part of the space race of the 1960s, to the point where students today are actively discouraged from considering STEM curriculums and careers by counselors and parents. Sadly, there is a perception that such educations do not lead to successful careers and financial stability.

There is some movement on this front, but much more needs to be done, particularly at the K-12 levels. Because of the cultural leaps and bounds that technology has afforded the post-boomer generations, we believe that more attention should be given to the use of that technology to communicate with and engage students. Many programs rely upon traditional mentor-protégé arrangements at the secondary and post-secondary levels. While these programs are effective, they are also limited in scale and numbers; too limited to meet the needs of our nation. Impressions are formed far earlier in the formative mind and we must engage students through technology at an early age for STEM careers.

In the near term, we encourage the Subcommittee to express support for reauthorization of the America Competes Act as an incubator for education programs in STEM. We also ask that Congress support the large increases in basic research in the FY2011 budget proposal, which will help spur the next wave of America innovation and train the next generation of scientists, technologists, engineers and mathematicians. For DoD, that is an increase of about 16% to $1,999 million.[7] Congress must contribute to a national effort to encourage students to pursue STEM educations.

Research & Development

[7] Task Force on American Innovation

A stronger, permanent R&D tax credit is still a badly needed incentive for spurring future research and development in the United States. Companies cannot adequately depend on credits that expire, making temporary credits an ineffective incentive for the technology industry. By comparison to other countries where R&D incentives are far more compelling, the United States is losing its ability to attract research and development activities to its shores.

In the near term, we encourage the Subcommittee to express support for reauthorization of the America Competes Act as an incubator for education programs in STEM. We also ask that Congress support the large increases in basic research in the FY2011 budget proposal, which will help spur the next wave of America innovation and train the next generation of scientists, technologists, engineers and mathematicians. For DoD, that is an increase of about 16% to $1,999 million.[8] It has been many years since Government played a significant role in research & development and these increases are an encouraging sign that trend may be reversed.

Cybersecurity and Information Assurance

Threat Sharing

TechAmerica has for some time now expressed concerns about the incomplete dialogue that DoD has with industry regarding IA threats. Historically, their focus has been on the systems integrator community (defined as the Defense Industrial Base or DIB) and, while those companies are members of TechAmerica and an indispensible community to engage for any discussions on IA threats, the vast majority of the tech sector is not formally engaged in threat sharing activities with DoD. Such a lack of dialogue leaves an incomplete picture for both the Department and industry. It is difficult to envision a thorough discussion on IA threats when commercial software developers and original equipment manufacturers are not formally part of the conversation.

Recently, the Department extended the Defense Industrial Base initiative (DIB/IA), which heretofore been a relatively limited effort to protect unclassified DoD information that resides or transit on a DIB information system or network through the release of Instruction 5205.13. This memorandum assigns responsibilities for fourteen separate DoD entities and subagencies and will have a broad and significant

[8] Task Force on American Innovation

DRAFT

impact on industry and its' ability support the Department to meet mission goals. As noted above, it is our hope that the Department will engage all of industry to effectively implement this new effort.

To promote a more robust and thorough dialogue and better protect the security interests and infrastructure of the National Security community, TechAmerica would recommend that the Subcommittee consider developing report language for the FY11 Defense Authorization Act. That language would require the expansion of DoD's threat sharing activities to formally include all of the industry elements comprising the tech sector as part of the implementation activities of Instruction 5205.13.

Certification & Accreditation

In July of last year, TechAmerica applauded the release of a Memorandum establishing reciprocity for certification and accreditation (C & A) for information systems across the Department. Industry has long had concerns about the lack of coordination between the C & A processes at DoD, particularly when companies would be forced to test the same device to the same or very similar standards or criteria for different testing entities. Such testing is frequently very expensive for companies and can take months to complete. Repetitive testing also delays the acquisition of technology products, frequently delivering second or third generation old products to the warfighter. It is our hope that the Department will engage industry to participate in the development of a reciprocally accepted C & A process and a DoD APL. We also hope that the Subcommittee will monitor this process as it develops to ensure that services and agencies do not seek to preserve independent certification and accreditation processes, thereby negating any efficiencies that reciprocity would have achieved.

Global Supply Chain Assurance

In 2007, TechAmerica collaborated with the Center for Strategic and International Studies to release a report[9] regarding industry recommendations for demonstrating assurance in the global supply chain. Those recommendations are still valid in this discussion. They include:

1. Assess the risk (and share the assessment). Inserting malicious code into software during the production process (whether overseas or in the United States) is only one of several attack options available to opponents.

[9] Foreign Influence on Software: Risks and Recourse, CSIS, March 2007

DRAFT

Responsibility for collecting information about opponents who are considering such attacks and the form these attacks might take should be assigned to the Intelligence Community, and the information shared among agencies and with appropriately cleared company representatives. Government and industry can develop formal processes to improve the exchange of information about threats and vulnerabilities to inform and coordinate their risk assessments.

2. Focus on assurance, not location. In the past, it was safe to assume that technology produced in the United States by a U.S. firm did not contain intentional vulnerabilities. This assumption no longer holds. Even if the technology is manufactured in the United States, the global nature of business means that this alone does not guarantee trustworthiness. An American company is likely to have employees from a broad range of countries. Foreign intelligence agencies could take advantage of the increasing internationalization of business to insert or recruit insiders, including U.S. citizens, with access to software production in the United States. Moreover, the borderless nature of information networks – one of its great attributes – means that malicious actors can be anywhere to access their targets anywhere, even in the U.S., if the appropriate protections are not in place.

The place where companies make software is not the key variable. Since 2000, many companies have made security a central element of their design and production processes for software. A strategy that takes advantage of the best procedures adopted by leading software manufacturers to make their products more secure has a better chance of succeeding than a strategy that attempts to determine security by looking at location.

3. Avoid one-size-fits-all solutions. The government already has processes for producing software with high assurance levels for very sensitive applications, such as command-and-control or intelligence. Cleared personnel working in secure facilities and following strict guidelines write this software. This provides software that is more trustworthy, but it is too expensive and too limiting to scale across government.

Building on existing efforts, an effective strategy will map software assurance levels and requirements to the sensitivity of the function and networks they support. Federal requirements could scale progressively from routine applications to the most sensitive, with requirements increasing to match sensitivity.

DRAFT

4. Refocus and reform existing certification processes. There are already several security certification processes for software products, such as the Common Criteria, but these processes do not ensure that certified software products are capable of resisting hostile attack. The United States can lead an effort that engage the industry to streamline these certification processes, reduce their cost, and buttress them with best practices and software assurance tools.

5. Identify commercial-sector best practices and tools and expand their use. Many companies already have extensive software assurance procedures as part of their production processes. The processes include a sequence of internal reviews for performance and security, testing, external testing and red-teaming, and the use of software review tools (some commercial, some proprietary and developed by the software company itself) to find vulnerabilities or errors. These practices offer the building blocks for an approach that is most likely to succeed in reducing the risk of distributed production. Extending these best practices would improve software assurance and security overall and reduce risk from hidden malicious code.

As part of this effort, the government could provide incentives and support for building better software assurance tools. As software programs continue to grow in size, investment in R&D for better tools will become more important for preliminary checks of the millions of lines of code found in many products.

6. Create a governance structure (or structures) for assurance. Companies may be taking extensive steps to improve software assurance, but if these steps are unknown or unmeasured, they cannot increase trust. Finding ways to overcome this is a crucial step for increasing trust in software products used for national security and critical infrastructure applications. It is essentially a governance problem. Traditional approaches to governance—command-and-control or regulations—do not work as well as they once did, or they may increase assurance at an unacceptable cost. An alternative solution is to create public-private partnerships to improve assurance. Whether this structure is formal or informal (and there are a number of existing groups that could be consolidated to serve this purpose), the objective would be to identify and share the best practices developed by software companies and shape requirements and procedures for better software assurance.

7. Accelerate information assurance efforts. Even if there were no foreign participation in IT production, networks would still be insecure. Networks involve thousands of different devices, some running older legacy code, others

DRAFT

running unpatched programs, and all facing the possibility that they are vulnerable because of a configuration error found in a separate network to which they connect but do not control. In this environment, knowing who has accessed information, and whether they have changed it, copied it, or transferred it offers a more efficient way to improve security. Greater attention to accountability and transparency in information use—monitoring and safeguarding data at rest—can help manage risk. Emerging technologies for information assurance, use control, and better authentication and authorization can counterbalance network and software vulnerabilities by allowing networks to control who can access information and what they can see and do with it.

8. Promote leadership in IT innovation. Globalization and distributed production are unavoidable, but the United States can take steps to keep itself at the forefront of technology. Technological innovation is good for the economy and for national security. Innovation makes life more difficult for opponents. All of an opponent's work to "rig" one technology is wasted if a new technology appears and supplants it. Innovation can improve assurance processes, tools, and overall network and information security. Measures that improve the climate for innovation in the United States (such as increased funding for IT-related R&D) also help build a skilled domestic workforce, so that the United States does not find itself relegated to low-end functions or working off some other nation's designs.

TechAmerica members have identified over a dozen various efforts across the Federal government that are purported to be addressing aspects of assuring the global supply chain. An unavoidable element of the technology that the Department acquires and deploys on a daily basis is that it is sourced from a global industry. While industry is willing to help develop the mechanisms to provide greater assurance in the supply chain, government must commit to sharing the risks and liabilities as part of that effort. Several of the government efforts seek to revise the acquisition process to place liability – even unlimited liability – on the vendors of hardware, software or services. Such a lopsided assignment of risk is unworkable and would only serve to cut the government off from the critical technologies it needs. Industry believes a more workable framework for sharing risk will include a demonstration of assurance in the products and services offered to the government, coupled with revised acquisition behavior on the part of government procurers.

TechAmerica is leading the industry response to the Federal Acquisition Council regarding their proposal on supply chain assurance offered as an Advanced Notice of Proposed Rulemaking on "Authentic IT". While the FAR Council has held public

DRAFT

hearings and sought out industry participation in formulating a solution to this problem, other efforts have not been so transparent. A recent effort by the National Institute of Standards and Technology, with participation from DoD and DHS, among other agencies involved a draft Special Publication was not vetted with industry until almost ready for publication.

Industry is very concerned that without oversight and coordination, government risks creating multiple, potentially conflicting requirements for the demonstration of assurance for hardware, software and services. These conflicts could unintentionally prevent companies from bringing their innovations to the public sector market, create significant barriers for small and mid-sized companies or drive other companies from the market because of an inability to accept the financial ramifications on their business model. The Subcommittee should seek to encourage the Administration to identify a single authority to consolidate and coordinate the various efforts addressing this issue.

Legal Challenges

There are a number of laws and regulations that prohibit or discourage information sharing and operational collaboration between industry and government that are in need of attention from Congress. Many of our policies and their statutory foundations were crafted before the Internet was invented and certainly before it became the ubiquitous resource it is today. Others are unintentionally restrictive because the drafters could not contemplate the technologies and capabilities that we now enjoy in the age of innovation.

The Subcommittee should consider a review of relevant portions of Title 10 for such antiquated authorities that inhibit the ability of the National Security community to protect our Nation's information systems, infrastructure and networks. Additionally, the Subcommittee should consider coordinating with other committees to address similar disconnects between the United States and our global partners. Such an undertaking would not be easy, but will be a necessary endeavor if we are to have success securing Cyber space for our Nation.

DRAFT